(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 09218852 A

(43) Date of publication of application: 19.08.97

(51) Int. Cl G06F 15/00
G06F 1/00
G06F 13/00
G06F 13/00

(21) Application number: 08025456

(22) Date of filing: 13.02.96

(71) Applicant: FUJITSU F I P KK

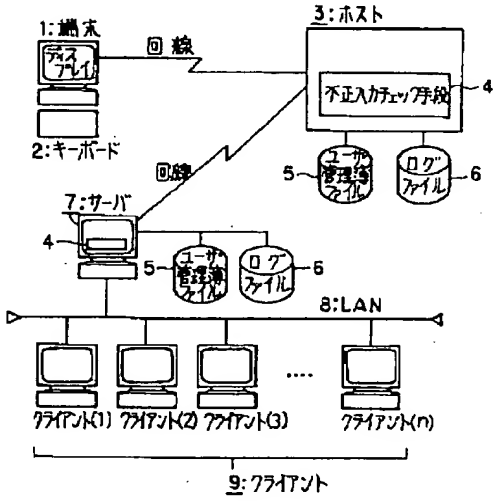
(72) Inventor: FUKUI TAKAMITSU

(54) ILLEGALITY CHECKING SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized use by reporting unauthorized access and an unauthorized character string to a normal user and making him/her change a password or the like.

SOLUTION: This system is provided with an unauthorized input checking means for retrieving a user management book 5 corresponding to the input of a user ID through a line, urging the input of the password when it is registered, repeating the storage of the inputted character string and the date and time of the input in a log file 6 and the urging of re-input when the inputted character string is not correct for the password registered corresponding to the user ID of the user management book 5, performing disconnection in exceeding the prescribed number of times, and on the other hand, when it is correct, connecting the line, displaying the previously stored incorrect unauthorized character string, date and time inside the log file 6 and displaying the log-out date and time of a previous time.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平9－218852

(43)公開日　平成９年(1997) ８月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｂ
	1/00	３７０			1/00	３７０Ｅ
	13/00	３５１			13/00	３５１Ｆ
		３５７				３５７Ｚ

審査請求　未請求　請求項の数４　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平8－25456

(22)出願日　平成８年(1996) ２月13日

(71)出願人　591106864
富士通エフ・アイ・ピー株式会社
東京都港区新橋５丁目36番11号

(72)発明者　福井　孝光
東京都港区新橋５丁目36番11号　富士通エフ・アイ・ピー株式会社内

(74)代理人　弁理士　岡田　守弘

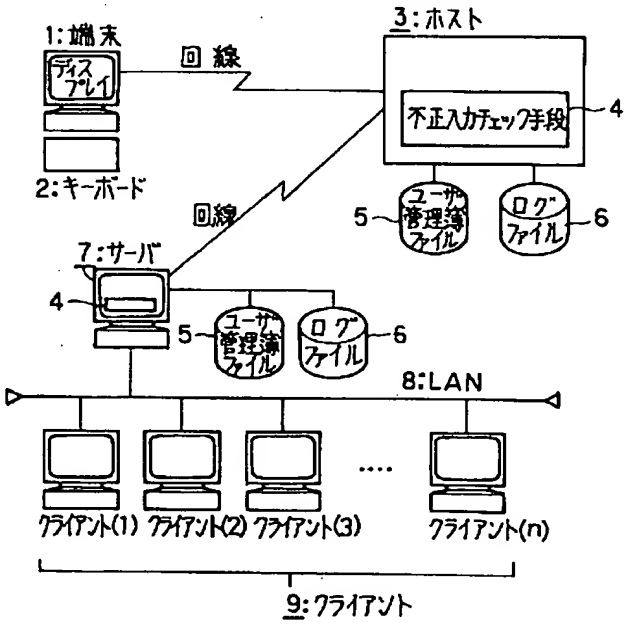
(54)【発明の名称】　不正チェックシステム

(57)【要約】

【課題】　本発明は、不正チェックシステムに関し、正規の利用者に不正アクセスおよび不正文字列を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることを目的とする。

【解決手段】　回線を介した利用者ＩＤの入力に対応してユーザ管理簿を検索して登録されているときに暗証番号の入力を促し、入力された文字列がユーザ管理簿の利用者ＩＤに対応づけて登録されている暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示する不正入力チェック手段とを備えるように構成する。

本発明のシステムブロック図



【特許請求の範囲】
【請求項１】回線を介したログインの不正チェックを行う不正チェックシステムにおいて、
利用者ＩＤに対応づけて暗証番号を登録するユーザ管理簿と、
回線を介した利用者ＩＤの入力に対応して上記ユーザ管理簿を検索して登録されているときに暗証番号の入力を促し、入力された文字列が上記ユーザ管理簿の上記利用者ＩＤに対応づけて登録されている暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示する不正入力チェック手段とを備えたことを特徴とする不正チェックシステム。
【請求項２】回線を介したログインの不正チェックを行う不正チェックシステムにおいて、
利用者ＩＤと暗証番号とを対応づけて登録するユーザ管理簿と、
回線を介した利用者ＩＤおよび暗証番号の入力に対応して上記ユーザ管理簿を検索して利用者ＩＤに対する暗証番号が正しくないときに入力を促し、入力された文字列が上記ユーザ管理簿の上記利用者ＩＤに対する暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示する不正入力チェック手段とを備えたことを特徴とする不正チェックシステム。
【請求項３】上記正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時の表示を、当該正しいときに回線接続の回数が所定回数を越えるまで繰り返し表示、あるいは当該正しいときに回線接続の日から所定日以前までのものを表示することを特徴とする請求項１あるいは請求項２記載の不正チェックシステム。
【請求項４】上記不正ログイン後あるいは不正ログインが所定回数越えたときに、所定期間の間、該当する利用者ＩＤのログインを許可しないことを特徴とする請求項１ないし請求項３記載のいずれかの不正チェックシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、回線を介したログインの不正チェックを行う不正チェックシステムに関するものである。
【０００２】
【従来の技術】従来、パソコン通信などでは、ログイン時に、「前回のログアウト日時」を下記のように表示し、第三者が本人になりすました利用がないかをチェックすることを行っていた。
【０００３】前回LOG OUT 95/09/10　10:11:12
【０００４】
【発明が解決しようとする課題】しかし、ログイン時に前回のログアウト日時が表示されても、第三者に不正使用されたかをチェックするには、自分の前回のログアウト日時を記憶してそれと比較して自分がアクセスした日時か、他人が不正にアクセスした日時かを判別する必要があり、確認が行い難いという問題があった。
【０００５】また、不正の第三者が他人の暗証番号を知るために、その本人の利用者番号（ＩＤ）を入力し、その後に、想定した暗証番号（パスワード）を入力してトライしても、通常は数回のトライで正しくないので通信が途絶（切断）される。しかし、再度異なる想定される暗証番号を入力してトライすることを繰り返しても、その不正トライの事実を本人が知ることができなかった。このために、他人の利用者番号（ＩＤ）に対して何度も暗証番号を入力してトライし、その暗証番号を探りだし、不正利用を許すことになってしまうという問題があった。
【０００６】また、金融機関では、第三者が不正利用の目的で、不正なパスワードが投入された場合、所定の回数を越えたときにカードなどを無効にし、再使用できないようにしてしまうため、度忘れしたり感違いして間違ったパスワードを繰り返し入力してしまった正規の利用者が利用できなくなる問題もあった。この際、パソコン通信などでは、不正利用を完全に無くすよりも、不正利用のトライがあったことを正規利用者に知らせたり、不正利用から守るようにしたりする工夫が望まれている。
【０００７】本発明は、これらの問題を解決するために、回線を介して入力された利用者ＩＤおよび暗証番号について間違った入力があったときに所定回数のリトライを許すと共に不正アクセスを記憶しておき、正常通信開始時に前回のログアウト日時と共に不正アクセスログを表示し、正規の利用者に不正アクセスおよび不正文字列を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることを目的としている。
【０００８】
【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、ホスト４は、端末１やサーバ７に接続して各種サービスを提供するものであって、ここでは、不正入力チェック手段４などから構成されるものである。
【０００９】不正入力チェック手段４は、ユーザ管理簿５を参照してログイン時の不正をチェックしたり、チェックして不正と判明したときに入力された文字列、日時などのログをログファイル６に格納したり、正常なログイン時に過去の不正な文字列、日時などを表示したりな

どするものである。

【００１０】サーバ７は、ＬＡＮ８に接続されたクライアントを統括管理するものであって、ここでは、不正入力チェック手段４などから構成されるものである。ユーザ管理簿ファイル５は、利用者ＩＤに対応づけて暗証番号を管理するものである。

【００１１】ログファイル６は、不正ログイン時に入力された文字列、日時などを保存するものである。次に、動作を説明する。

【００１２】不正入力チェック手段４が回線を介した利用者ＩＤの入力に対応してユーザ管理簿ファイル５を検索して登録されているときに暗証番号の入力を促し、入力された文字列がユーザ管理簿ファイル５の利用者ＩＤに対応づけて登録されている暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル６内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示するようにしている。

【００１３】また、不正入力チェック手段４が回線を介した利用者ＩＤおよび暗証番号の入力に対応してユーザ管理簿ファイル５を検索して利用者ＩＤに対する暗証番号が正しくないときに入力を促し、入力された文字列がユーザ管理簿ファイル５の利用者ＩＤに対する暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル６内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示するようにしている。

【００１４】これらの際に、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時の表示を、正しいときに回線接続の回数が所定回数を越えるまで繰り返し表示、あるいは正しいときに回線接続の日から所定日以前までのものを表示するようにしている。

【００１５】また、不正ログイン後あるいは不正ログインが所定回数越えたときに、所定期間の間、該当する利用者ＩＤのログインを許可しないようにしている。従って、回線を介して入力された利用者ＩＤおよび暗証番号について間違った入力があったときに所定回数のリトライを許すと共に不正アクセス時の文字列と日時などを不正アクセスログとして記憶しておき、正常通信開始時に前回のログアウト日時と共に不正アクセスログを表示することにより、正規の利用者に不正アクセスのあった旨を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることが可能となる。

【００１６】

【発明の実施の形態】次に、図１から図５を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１７】図１は、本発明のシステム構成図を示す。図１において、端末１は、回線を介してホスト４と接続し、各種業務処理を行うものであって、ここでは、ディスプレイ、キーボード２、処理装置などから構成されるものである。

【００１８】ホスト４は、回線を介して端末１およびサーバ７と接続し、各種サービスを提供するものであって、ここでは、不正入力チェック手段４などから構成されるものである。

【００１９】不正入力チェック手段４は、端末１やクライアント９などから回線を介して利用者ＩＤおよび暗証番号が入力があったときにユーザ管理簿５を参照してログインの不正をチェックしたり、チェックして不正と判明したときに入力された文字列、日時などのログをログファイル６に格納したり、正常なログイン時に過去の不正なログインされた文字列、日時などを表示したりなどするものである。

【００２０】ユーザ管理簿ファイル５は、利用者ＩＤと暗証番号とを対応づけて管理するものである（図３参照）。ログファイル６は、不正ログイン時に入力された文字列、日時などを保存するものである（図３参照）。

【００２１】サーバ７は、ＬＡＮ８を介して複数のクライアント９を統括制御および回線を介してホスト３に接続したりなどするものであって、ここでは、不正入力チェック手段４などから構成されるものである。

【００２２】ＬＡＮ８は、ローカルエリアネットワークであって、複数のクライアント（１）ないし（ｎ）およびサーバ７を相互に接続するものである。クライアント９は、クライアント（１）ないし（ｎ）から構成され、ＬＡＮ８を介して相互に接続およびサーバ７に接続、更にサーバ７経由でホスト３に接続し、各種業務処理を行うものである。

【００２３】次に、図２のフローチャートに示す順序に従い、図１の構成の動作を詳細に説明する。図２において、Ｓ１は、利用者番号（ＩＤ）の入力要求を行う。

【００２４】Ｓ２は、Ｓ１の入力要求に応じて、利用者が利用者番号を入力する。これは、例えば図１の端末１から回線を介してホスト３に接続し、端末１のディスプレイ上に表示された利用者番号（ＩＤ）の入力フィールドに利用者番号（ＩＤ）をキー入力する。

【００２５】Ｓ３は、ユーザ管理簿ファイルと照合する。これは、Ｓ２で入力された利用者番号（ＩＤ）を回線を介して受信したホスト３の不正入力チェック手段４がこの受信した利用者番号（ＩＤ）が、ユーザ管理簿ファイル５に登録されているか照合する。

【００２６】Ｓ４は、ＯＫか否かを判別する。ＹＥＳの場合には、利用者番号（ＩＤ）がユーザ管理簿ファイル５に登録されていると判明したので、Ｓ８に進む。一方、ＮＯの場合には、利用者番号（ＩＤ）がユーザ管理

簿ファイル５に登録されていないと判明したので、Ｓ５に進む。

【００２７】Ｓ５は、エラー回数がｎ回か判別する。ＹＥＳの場合には、トライ回数ｎの制限を越えたと判明したので、Ｓ７で切断する。一方、ＮＯの場合には、トライ回数ｎ以内と判明したので、Ｓ６で再入力要求を行い、Ｓ１以降を繰り返す。

【００２８】以上のＳ１からＳ７によって、利用者が図１の端末１を使ってホスト４に接続してログインするときに、利用者番号（ＩＤ）を入力してユーザ管理簿ファイル５に登録されているか否かを判別し、ＹＥＳのときにＳ８以降の処理に進み、ＮＯのときに回線を切断する。

【００２９】Ｓ８は、パスワード（暗証番号）の入力要求を行う。Ｓ９は、Ｓ８の入力要求に応じて、利用者がパスワードを入力する。これは、例えば図１の端末１から回線を介してホスト３に接続し、端末１のディスプレイ上に表示されたパスワードの入力フィールドにパスワードをキー入力する。

【００３０】Ｓ１０は、ユーザ管理簿ファイルと照合する。これは、Ｓ９で入力されたパスワードを回線を介して受信したホスト３の不正入力チェック手段４がこの受信したパスワードが、ユーザ管理簿ファイル５の利用者番号（ＩＤ）に対応づけて登録されているか照合する。

【００３１】Ｓ１１は、ＯＫか否かを判別する。ＹＥＳの場合には、パスワードがユーザ管理簿ファイル５の利用者番号（ＩＤ）に対応づけて登録されていると判明したので、Ｓ１７に進む。一方、ＮＯの場合には、パスワードがユーザ管理簿ファイル５の利用者番号（ＩＤ）に対応づけて登録されていないと判明したので、Ｓ１５に進む。

【００３２】Ｓ１２は、エラー回数がｍ回か判別する。ＹＥＳの場合には、トライ回数ｍの制限を越えたと判明したので、Ｓ１５で異常アクセスを記録し、Ｓ１６で回線切断する。例えば異常アクセスしたパスワードの文字列および日時などをログファイル６に、利用者番号（ＩＤ）に対応づけて保存する。一方、Ｓ１２のＮＯの場合には、トライ回数ｍ以内と判明したので、Ｓ１４で再入力要求を行い、Ｓ８以降を繰り返す。

【００３３】以上のＳ８からＳ１６によって、利用者が図１の端末１を使ってホスト４に接続してログインするときに、利用者番号（ＩＤ）がＳ４のＹＥＳでＯＫとなったときに、パスワードを入力してユーザ管理簿ファイル５に利用者番号（ＩＤ）に対応づけてパスワードが登録されているか否かを判別し、ＹＥＳのときにＳ１７以降の処理に進み、ＮＯのときに異常アクセス記録をログファイル６に保存した後、回線を切断する。

【００３４】Ｓ１７は、エラー情報ありか判別する。これは、Ｓ１５の異常アクセス記録がログファイル６に当該利用者番号（ＩＤ）に対応づけて保存されているか判別する。ＹＥＳの場合には、Ｓ１８ないしＳ２０の処理を行う。一方、Ｓ１７のＮＯの場合には、異常アクセスが保存されていないと判明したので、Ｓ２１の通常処理へ進む。

【００３５】Ｓ１８は、エラー内容を表示する。これは、Ｓ１７のＹＥＳでエラー情報がログファイル６に保存されていると判明したので、エラー内容を表示、例えば後述する図５に示すように、不正パスワード、日時、文字列などを表示する。

【００３６】Ｓ１９は、エラー表示クリアか判別する。これは、Ｅｒｒ　ｆｌｇ　ｏｆｆ（エラーフラグがＯＦＦ）か判別する。ＹＥＳの場合には、Ｓ２０でエラー表示クリアを行い、Ｓ２１に進む。Ｓ１９のＮＯの場合には、Ｓ２１に進む。

【００３７】Ｓ２１は、通常処理へ進む。これは、正規の利用者が端末１を操作してホスト３に回線を介して接続できたので、利用者が端末１を操作してホスト３からの各種サービスの提供を受ける。

【００３８】尚、不正ログイン（利用者ＩＤがＯＫとなったがパスワードが正しくないこと）が所定回数を越えたときに、所定期間の間、該当する利用者ＩＤのパスワードを入力したログインを許可しないようにし、１つの利用者ＩＤに対するパスワードを繰り返し試して探索する事態を防止するようにしてもよい。

【００３９】図３は、本発明のファイル例を示す。図３において、ユーザ管理ファイル５は、利用者のＩＤ番号に対応づけてパスワード、異常フラグ（Ｅｒｒ　ｆｌｇ）、ログ位置などを登録するものである。ここで、異常フラグが異常があったときにＯＮに設定して正規の利用者がホスト３に接続（ログイン）したときに端末１の画面上にエラー情報（図５参照）を表示するためのものである。異常フラグがＯＦＦのときは端末１の画面上にエラー情報を表示しない。

【００４０】ログファイル６は、異常アクセスの情報を保存するものであって、ここでは、図示のように、日単位に１回目、２回目・・・のときの時刻および文字列を登録したものである。ここでは、例えば１９９４年１１月０７日の１回目の時刻が１２時４３分５１秒で不正パスワードとして入力された文字列が“Ｔ－ＦＵＫＵＩＺ”である。以下同様に、図示のように保存する。

【００４１】図４は、本発明の動作説明フローチャート（その２）を示す。図４において、Ｓ３１は、利用者が端末１を操作して回線を介してホスト３に接続する。

【００４２】Ｓ３２は、利用者がＩＤ（利用者ＩＤ）を入力してホスト３に通知する。Ｓ３３は、登録済みか判別する。これは、ホスト３の不正入力チェック手段４がＳ３２で通知された利用者ＩＤがユーザ管理簿ファイル５に登録されているか判別する。ＹＥＳの場合には、利用者ＩＤが登録されていると判明したので、Ｓ３６に進む。一方、ＮＯの場合には、Ｓ３４で所定回数以内のリ

トライか判別する。ＹＥＳの場合には、Ｓ３２に戻り繰り返す。一方、ＮＯの場合には、Ｓ３５で切断する。

【００４３】以上のＳ３１からＳ３５によって、利用者が端末１から正規の利用者ＩＤを入力し、回線を介してホスト３に通知すると、ホスト３の不正入力チェック手段４がユーザ管理簿ファイル５に登録済みのときにＳ３６のパスワードの入力に進み、一方、登録されていないときにリトライが所定回数を越えたときに回線を切断する。

【００４４】Ｓ３６は、利用者がパスワードを入力する。Ｓ３７は、正しいか判別する。これは、利用者が図１の端末１を操作してパスワードを入力して回線を介してホスト３の不正入力チェック手段４に通知し、当該不正入力チェック手段４がユーザ管理簿ファイル５の利用者ＩＤに対応づけて登録されているパスワードと一致（正しい）か判別する。ＹＥＳの場合には、パスワードが正しいと判明したので、Ｓ４１に進む。一方、ＮＯの場合には、Ｓ３８に進む。

【００４５】Ｓ３８は、データログする。これは、不正のパスワード、日時などをログファイル６に図３に示すように保存する。Ｓ３９は、所定回数内か判別する。これは、パスワードの入力が所定回数以内でリトライの制限範囲内か判別する。ＹＥＳの場合には、Ｓ３６に戻り、利用者にパスワードの入力を促して入力させることを繰り返す。一方、ＮＯの場合には、Ｓ４０で回線を切断する。

【００４６】以上のＳ３６からＳ４０によって、利用者が端末１から正規のパスワードを入力し、回線を介してホスト３に通知すると、ホスト３の不正入力チェック手段４がユーザ管理簿ファイル５に利用者ＩＤに対応づけてパスワードが登録されていたときにＳ４１に進み、一方、登録されていないときにデータログ（不正パスワードの文字列、日時など）を保存およびリトライが所定回数を越えたときに回線を切断する。

【００４７】Ｓ４１は、不正データが有りか判別する。これは、既述した図３のユーザ管理簿ファイル５中の利用者ＩＤに対応する異常フラグがＯＮであって、ログファイル６中に異常アクセス情報（日時と不正パスワードとして入力された文字列など）が保存されているか判別する。ＹＥＳの場合には、Ｓ４２に進む。ＮＯの場合には、Ｓ４６で通常処理へ進む。

【００４８】Ｓ４２は、不正データありのメッセージを表示する。これは、端末１の画面上に不正データありのメッセージを表示し、正規の利用者に不正データ（不正パスワードとして入力された文字列と日時など）がある旨のメッセージを表示する。

【００４９】Ｓ４３は、詳細表示するか判別する。これは、利用者から詳細表示の指示があったか判別する。ＹＥＳの場合には、Ｓ４４に進む。ＮＯの場合には、Ｓ４６で通常処理へ進む。

【００５０】Ｓ４４は、Ｓ４３で詳細表示すると判明したので、詳細情報（図３のログファイル６の該当するエントリの内容）を表示する。Ｓ４５は、ログファイルをクリアする。これは、既述した図３のユーザ管理ファイル５中の異常フラグをＯＦＦにし、ログファイルの内容が表示済みを設定する。

【００５１】Ｓ４６は、通常処理へ進む。図５は、本発明の表示例（パスワード入力エラー情報表示例）を示す。これは、図１の端末１の画面上に表示したパスワード入力時のエラー情報の表示例である。以下画面上のデータを順次説明する。

【００５２】・第１行目の

>User-ID ----→AAA00001

は、利用者が入力した利用者ID"AAA00001"を表す(図３のユーザ管理簿ファイル５の１行目の利用者ＩＤ"AAA00001"に対応してここでは、正しいと判明する。

【００５３】・第２行目の

>Password ----→

は、利用者が入力したパスワード（画面上には盗用を考慮して非表示）であって、ここでは、"T-FUKUI"と入力されたとすると、図３のユーザ管理簿ファイル５の１行目の利用者ＩＤ"AAA00001"に対応した正しいパスワード"T-FUKUI"が入力されたこととなる。

【００５４】①は、前回のＬＯＧ　ＯＵＴ時刻を表示し、他人によって不正利用されていなかを、利用者に認識させるためのものである。②は、不正なパスワードの入力があったときに表示されるものであって、ここでは、図示のように、“不正なパスワードが入力された情報があります”というメッセージおよび詳細情報表示（１：する　２：しない）の選択番号を表示したものである。ここでは、“１（する）”を選択している。

【００５５】③は、②で“１（する）”を選択したことに対応して、エラー情報の詳細が表示されたものである（図３の正規の利用者ＩＤおよびパスワードに対応づけてログファイル６に保存されているエラー情報の詳細を表示したものである。この詳細情報の表示は、予め指定した所定日数前から現在のものを表示したり、所定日までのものを表示したり、所定回数を越えるまで表示したり、任意に表示する。ここでは、例えば第１行目のように、

・不正パスワードの入力日時“１９９４年１１月０７日　１２時４３分５１秒”　不正文字列“Ｔ－ＦＵＫＵＩＺ”

を表示する。

【００５６】尚、本実施例では、図２および図４では、利用者ＩＤが入力されてＯＫとなったときに次にパスワードが入力されてＯＫとなったときに正常運用へ進み、パスワードが入力されてＮＧのときに異常アクセス情報をログしたけれども、この順序に限られることなく、利用者が端末１の画面上で利用者ＩＤおよびパスワードの

両者を入力してホスト３に通知し、ユーザ管理簿ファイル５を参照して利用者ＩＤおよびパスワードの正当性をどのような順番で判別するようにしてもよい。

【００５７】

【発明の効果】以上説明したように、本発明によれば、回線を介して入力された利用者ＩＤおよび暗証番号について間違った入力があったときに所定回数のリトライを許すと共に不正アクセス時の文字列と日時などを不正アクセスログとして記憶しておき、正常通信開始時に前回のログアウト日時と共に不正アクセスログを表示する構成を採用しているため、正規の利用者に不正アクセスのあった旨を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることができる。これらにより、

（１）　パソコン通信などにおいて、第三者が不正アクセスしようとしていることを、正規の利用者である本人に通知することができる。

【００５８】（２）　パソコン通信などにおいて、本人が間違って本人の利用者ＩＤを入力したり、パスワードを間違って入力したりしても、銀行のカードのように使用不可に書き替えてしまい、業務ができなくなるという事態の発生を無くすことができる。

【００５９】（３）　パソコン通信などにおいて、他人が不正アクセスしようとしている事実を正規の本人に知らせたり、その不正アクセスの日単位のアクセス回数や不正アクセス時の文字列のログを表示して知らせたりすることができる。

（４）　不正アクセス時の文字列を見た利用者は、盗用しようとしたパスワードの文字列を知り、これから容易に盗用できない文字列のパスワードに定期的に変えたりし、未然にパスワードの盗用による不正アクセスを防止できる。

【図面の簡単な説明】

【図１】本発明のシステムブロック図である。

【図２】本発明の動作説明フローチャート（その１）である。

【図３】本発明のファイル例である。

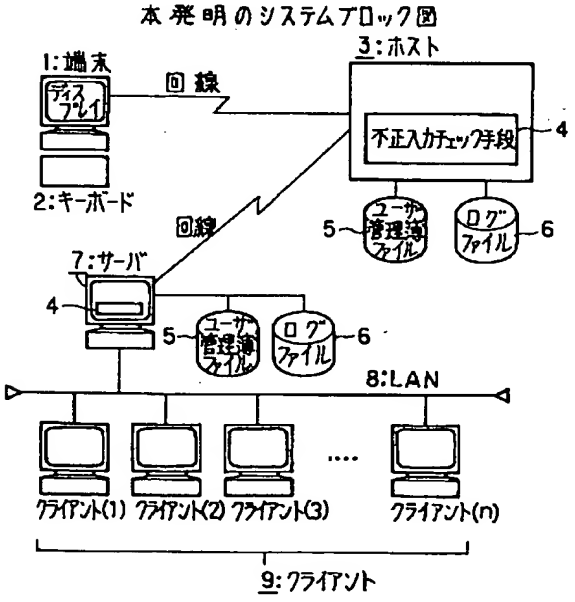
【図４】本発明の動作説明フローチャート（その２）である。

【図５】本発明の表示例である。

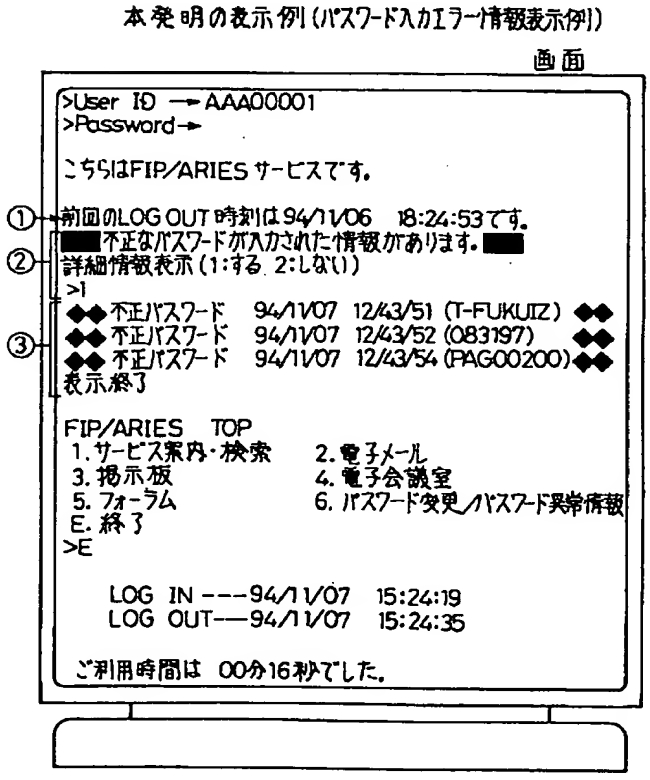
【符号の説明】

１：端末
２：キーボード
３：ホスト
４：不正入力チェック手段
５：ユーザ管理簿ファイル
６：ログファイル
７：サーバ
８：ＬＡＮ
９：クライアント

【図１】

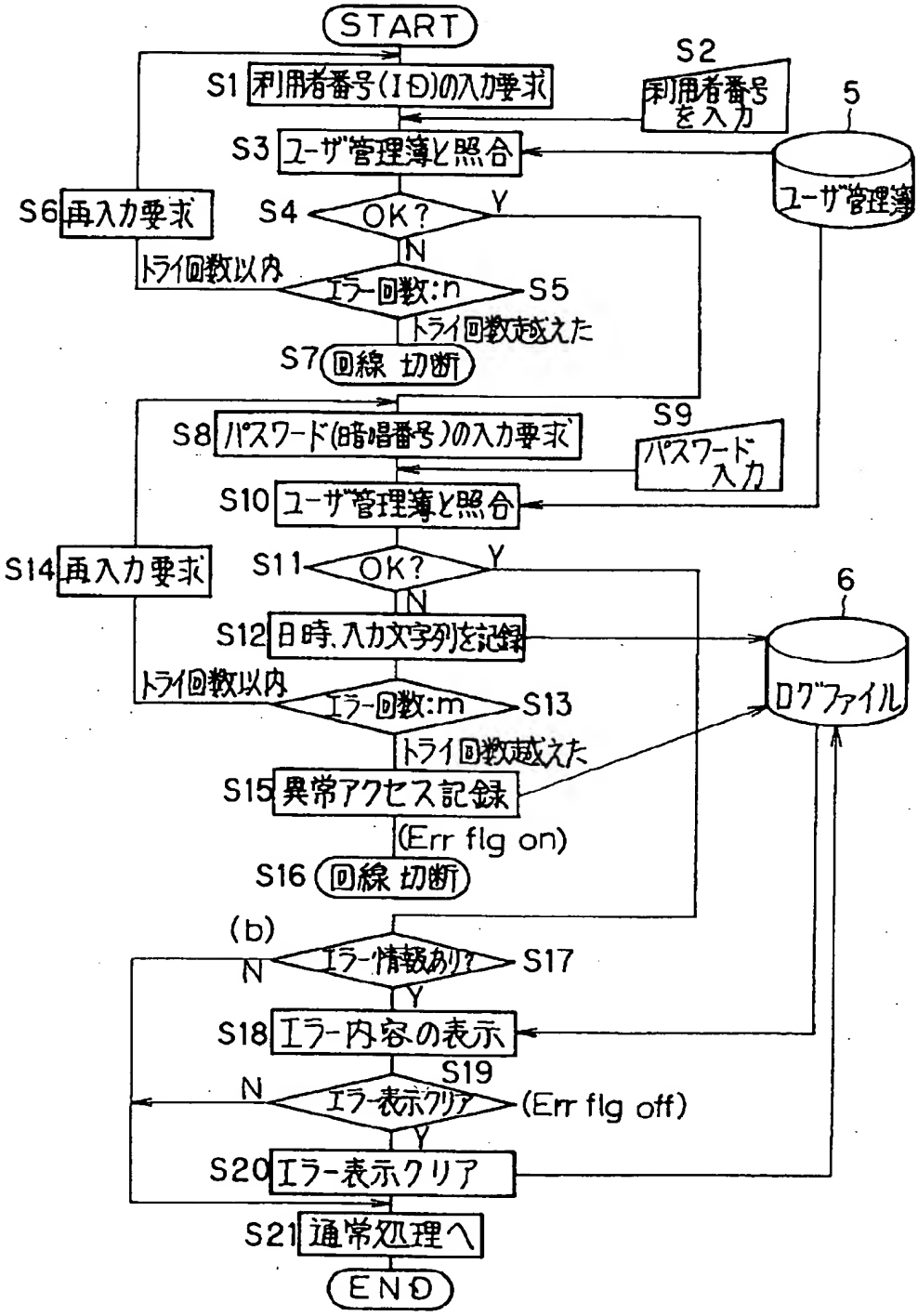


【図５】



【図２】

本発明の動作説明フローチャート（その１）



【図３】

本発明のファイル例

5:ユーザ管理簿ファイル

ID番号	パスワード		異常	ログ位置
AAA00001	T-FUKUI		E	000001
AAA00002	082197		N	

6:ログファイル

000001

日付け	時刻	1回	時刻	2回	時刻	3回	続き
94/11/07	12:43:51	T-FUKUIZ	12:43:52	083197	12:43:54	PAG00200	00000

【図４】

本発明の動作説明フローチャート(その2)